FINITE FIELDS AND THEIR APPLICATIONS 1, 102–114 (1995)

A Unified Approach to the Analysis of Compound Pseudorandom Numbers

JÜRGEN EICHENAUER-HERRMANN

Fachbereich Mathematik, Technische Hochschule Darmstadt, Schloßgartenstraße 7, D-64289 Darmstadt, Germany

Communicated by Peter Jau-Shyong Shiue

Received March 14, 1994

The present paper deals with a general compound method for generating uniform pseudorandom numbers. Equidistribution and statistical independence properties of the generated sequences are studied based on the discrepancy of certain point sets. A unified approach to the analysis of the full period and of (relatively large) parts of the period is worked out, which rests on bounds for certain exponential sums over finite fields. This calculus is applied to the compound nonlinear congruential mehod and to the compound explicit inversive congruential method, which have been introduced recently. Known upper bounds for the discrepancy over the full period are improved and new upper bounds for the discrepancy over parts of the period are established. © 1995 Academic Press, Inc.

1. INTRODUCTION

Nonlinear congruential methods of generating uniform pseudorandom numbers in the interval [0, 1) have been studied intensively during the last years. A review of the development of this important area can be found in the survey articles [2, 5, 8, 14–17, 19, 20] and in the excellent monograph of Niederreiter [18]. The generated sequences show several very attractive properties. However, in order to obtain a sufficiently large period length, it is necessary to perform all integer computations in multiprecision. Therefore, compound versions of some nonlinear congruential methods have been introduced [4, 7] which overcome this disadvantage. In the present paper the following general compound method is studied.

Let $p_1, \ldots, p_r$ be distinct primes and $i \in \{1, \ldots, r\}$. Identify

1071-5797/95 $6.00

$\mathbb{Z}_{p_i} = \{0, 1, \ldots, p_i - 1\}$ with the finite field of order p_i. Let $(y_n^{(i)})_{n\geq 0}$ be a sequence of elements of $\mathbb{Z}_{p_i}$, which is purely periodic with period length p_i. Let $(x_n^{(i)})_{n\geq 0}$ with

$$x_n^{(i)} = y_n^{(i)}/p_i \in [0, 1), \qquad n \geq 0,$$

be the corresponding stream of *pseudorandom numbers*. A sequence $(x_n)_{n\geq 0}$ of *compound pseudorandom numbers* in the interval [0, 1) is defined by

$$x_n \equiv x_n^{(1)} + \cdots + x_n^{(r)} \pmod 1, \quad n \geq 0.$$

Straightforward arguments show that the sequence $(x_n)_{n\geq 0}$ is purely periodic with period length $m = p_1 \cdot \ldots \cdot p_r$. Hence, in the compound method a very large period length m can be obtained, although exact integer computations have to be performed only in $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}$. The compound method was motivated by a similar approach for linear congruential generators in [21].

Equidistribution and statistical independence properties of the generated sequences, which are very important for their usability in a stochastic simulation, can be analyzed based on the discrepancy of s-tuples of successive pseudorandom numbers with $s = 1$ and $s \geq 2$, respectively. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^s$ the *discrepancy* is defined by

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^s$, $F_N(J)$ is N^{-1} times the number of points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the s-dimensional volume of J. Observe that the discrepancy of N true random points in $[0, 1)^s$ is almost always of an order of magnitude $N^{-1/2}(\log\log N)^{1/2}$ according to the law of the iterated logarithm for discrepancies [1, 11]. Subsequently, the abbreviations

$$\mathbf{x}_n = (x_{sn}, x_{sn+1}, \ldots, x_{sn+s-1}) \in [0, 1)^s, \qquad n \geq 0,$$

and

$$D_N^{(s)} = D_N(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1})$$

are used. In Section 4, upper bounds for the discrepancy $D_m^{(s)}$ over the full period and for the discrepancy $D_N^{(s)}$ over parts of the period $N < m$ are established, which depend on exponential sums over the finite fields $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}$. These exponential sums are introduced and analyzed in

Section 3. The reader is referred to [12] for an introduction to the theory of exponential sums. Section 2 contains some known auxiliary results. In Section 5, the main results are applied to the analysis of the compound methods in [4, 7].

2. Auxiliary Results

First, some further notation is necessary. For integers $k \geq 1$ and $q \geq 2$ let $C_k(q)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbb{Z}^k$ with $-q/2 < h_j \leq q/2$ for $1 \leq j \leq k$. Define

$$r(h, q) = \begin{cases} q \sin(\pi |h|/q), & \text{for } h \in C_1(q), \\ 1, & \text{for } h = 0, \end{cases}$$

and

$$r(\mathbf{h}, q) = \prod_{j=1}^{k} r(h_j, q)$$

for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(q)$. For real t the abbreviation $e(t) = e^{2\pi i t}$ is used, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$. Subsequently, a known general result for estimating discrepancies is stated which follows from [18, Thm. 3.10].

Lemma 1. *Let $N \geq 1$ and $q \geq 2$ be integers. Let $\mathbf{t}_n = \mathbf{y}_n/q \in [0, 1)^k$ with $\mathbf{y}_n \in \{0, 1, \ldots, q-1\}^k$ for $0 \leq n < N$. Then the discrepancy of the points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ satisfies*

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) \leq \frac{k}{q} + \frac{1}{N} \sum_{\mathbf{h} \in C_k(q)} \frac{1}{r(\mathbf{h}, q)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right|.$$

The following result is cited from [10, Lemma 3] and can be used for estimating the discrepancy over parts of the period.

Lemma 2. *Let $q \geq 1$ be an integer. Let $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{q-1} \in [0, 1)^k$ and define $\tilde{\mathbf{t}}_n = (\mathbf{t}_n, n/q) \in [0, 1)^{k+1}$ for $0 \leq n < q$. Then*

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) \leq \frac{q}{N} D_q(\tilde{\mathbf{t}}_0, \tilde{\mathbf{t}}_1, \ldots, \tilde{\mathbf{t}}_{q-1})$$

for $1 \leq N \leq q$.

The following result can be deduced from [4, Proof of Thm. 1; 7, Proof of Thm. 1].

LEMMA 3. *Let $q \geq 2$ be an integer. Then*

$$\sum_{\substack{\mathbf{h} \in C_k(q) \\ \mathbf{h} \equiv \mathbf{0} \pmod{d}}} \frac{1}{r(\mathbf{h}, q)} < \frac{1}{d} \left(\frac{2}{\pi} \log q + \frac{7}{5} \right)^k$$

for any divisor d of q with $1 \leq d < q$.

3. EXPONENTIAL SUMS

Lemmas 1 and 2 show that a crucial role for the analysis of the discrepancy $D_N^{(s)}$ is played by the *exponential sums*

$$S(\tilde{\mathbf{h}}) = \sum_{n=0}^{m-1} e(\tilde{\mathbf{h}} \cdot \tilde{\mathbf{x}}_n), \qquad \tilde{\mathbf{h}} \in \mathbb{Z}^{s+1},$$

where the points $\tilde{\mathbf{x}}_n$ for $0 \leq n < m$ are given by

$$\tilde{\mathbf{x}}_n = (\mathbf{x}_n, \ n/m) \in [0, 1)^{s+1}.$$

Let $i \in \{1, \ldots, r\}$ and define

$$\mathbf{x}_k^{(i)} = (x_{sk}^{(i)}, x_{sk+1}^{(i)}, \ldots, x_{sk+s-1}^{(i)}) \in [0, 1)^s, \qquad k \geq 0,$$
$$\tilde{\mathbf{x}}_k^{(i)} = (\mathbf{x}_k^{(i)}, k/p_i) \in [0, 1)^{s+1}, \qquad k \in \mathbb{Z}_{p_i},$$

and corresponding *exponential sums* over the finite field $\mathbb{Z}_{p_i}$

$$S_i(\tilde{\mathbf{h}}) = \sum_{k \in \mathbb{Z}_{p_i}} e(\tilde{\mathbf{h}} \cdot \tilde{\mathbf{x}}_k^{(i)}), \qquad \tilde{\mathbf{h}} \in \mathbb{Z}^{s+1}.$$

Observe that $S_i(\tilde{\mathbf{h}}) = p_i$ for all $\tilde{\mathbf{h}} \in \mathbb{Z}^{s+1}$ with $\tilde{\mathbf{h}} \equiv \mathbf{0} \pmod{p_i}$. Let $m_i = m/p_i$ and define $q_i \in \mathbb{Z}_{p_i}$ by $q_i \equiv m_i^{-1} \pmod{p_i}$.

LEMMA 4. *Let $\tilde{\mathbf{h}} = (\mathbf{h}, h_{s+1}) \in \mathbb{Z}^{s+1}$. Then*

$$S(\tilde{\mathbf{h}}) = \prod_{i=1}^{r} S_i(\mathbf{h}, h_{s+1} q_i).$$

Proof. Observe that

$$\mathbf{x}_n \equiv \sum_{i=1}^{r} \mathbf{x}_n^{(i)} \pmod 1, \qquad n \geq 0,$$

and hence

$$S(\tilde{\mathbf{h}}) = \sum_{n=0}^{m-1} e(\mathbf{h} \cdot \mathbf{x}_n + h_{s+1} n/m)$$

$$= \sum_{n=0}^{m-1} e\left(\sum_{i=1}^{r} \mathbf{h} \cdot \mathbf{x}_n^{(i)} + h_{s+1} n/m\right).$$

Now, the Chinese Remainder Theorem implies that

$$S(\tilde{\mathbf{h}}) = \sum_{\substack{(k_1,\cdots,k_r)\in \mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r} \\ n\equiv k_i \pmod{p_i},\ 1\leq i\leq r}} e\left(\sum_{i=1}^{r} \mathbf{h} \cdot \mathbf{x}_n^{(i)} + h_{s+1} n/m\right)$$

$$= \sum_{\substack{(k_1,\ldots,k_r)\in \mathbb{Z}_{p_1}\times\ldots\times\mathbb{Z}_{p_r} \\ n\equiv m_1 q_1 k_1 + \cdots + m_r q_r k_r \pmod m}} e\left(\sum_{i=1}^{r} \mathbf{h} \cdot \mathbf{x}_n^{(i)} + h_{s+1} n/m\right).$$

Since the sequence $(\mathbf{x}_n^{(i)})_{n\geq 0}$ is p_i periodic, one obtains

$$S(\tilde{\mathbf{h}}) = \sum_{(k_1,\ldots,k_r)\in \mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}} e\left(\sum_{i=1}^{r} \mathbf{h} \cdot \mathbf{x}_{k_i}^{(i)} + \sum_{i=1}^{r} h_{s+1} m_i q_i k_i/m\right)$$

$$= \sum_{(k_1,\ldots,k_r)\in \mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}} e\left(\sum_{i=1}^{r} (\mathbf{h} \cdot \mathbf{x}_{k_i}^{(i)} + h_{s+1} q_i k_i/p_i)\right)$$

$$= \sum_{(k_1,\ldots,k_r)\in \mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}} e\left(\sum_{i=1}^{r} (\mathbf{h}, h_{s+1} q_i) \cdot \tilde{\mathbf{x}}_{k_i}^{(i)}\right)$$

$$= \sum_{(k_1,\ldots,k_r)\in \mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_r}} \prod_{i=1}^{r} e((\mathbf{h}, h_{s+1} q_i) \cdot \tilde{\mathbf{x}}_{k_i}^{(i)})$$

$$= \prod_{i=1}^{r} \sum_{k_i\in\mathbb{Z}_{p_i}} e((\mathbf{h}, h_{s+1} q_i) \cdot \tilde{\mathbf{x}}_{k_i}^{(i)})$$

$$= \prod_{i=1}^{r} S_i(\mathbf{h}, h_{s+1} q_i). \quad \blacksquare$$

4. Discrepancy Bounds

In the present section upper bounds for the discrepancy $D_N^{(s)}$ of compound pseudorandom numbers over the full period $N = m$ and over (relatively large) parts of the period $N < m$ are established. These bounds only depend on upper bounds for the absolute value of the exponential sums $S_i(\tilde{\mathbf{h}})$ over the finite field $\mathbb{Z}_{p_i}$ for $1 \le i \le r$.

THEOREM 1. *Suppose that* $|S_i(\mathbf{h}, 0)| \le B_i$ *for any* $\mathbf{h} \in \mathbb{Z}^s$ *with* $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ *and* $1 \le i \le r$. *Then the discrepancy* $D_m^{(s)}$ *of s-tuples (over the full period) in the compound method satisfies*

$$D_m^{(s)} < \frac{1}{m} \prod_{i=1}^{r} (B_i + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s.$$

Proof. First, Lemma 1 is applied with $k = s$, $N = q = m$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \le n < m$. This yields

$$\begin{aligned} D_m^{(s)} &\le \frac{s}{m} + \frac{1}{m} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \left| \sum_{n=0}^{m-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \\ &= \frac{s}{m} + \frac{1}{m} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} |S(\mathbf{h}, 0)| \\ &= \frac{s}{m} + \frac{1}{m} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \prod_{i=1}^{r} |S_i(\mathbf{h}, 0)|, \end{aligned}$$

where the last equality follows from Lemma 4. Hence, one obtains

$$D_m^{(s)} \le \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1, \ldots, r\} \\ |I| < r}} \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i},\ i \in I \\ \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i},\ i \notin I}} \frac{1}{r(\mathbf{h}, m)} \prod_{i=1}^{r} |S_i(\mathbf{h}, 0)|$$

$$\le \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1, \ldots, r\} \\ |I| < r}} \prod_{i \in I} p_i \prod_{i \notin I} B_i \sum_{\substack{h \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i},\ i \in I \\ \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i},\ i \notin I}} \frac{1}{r(\mathbf{h}, m)}$$

$$\le \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1, \ldots, r\} \\ |I| < r}} \prod_{i \in I} p_i \prod_{i \notin I} B_i \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i},\ i \in I}} \frac{1}{r(\mathbf{h}, m)}.$$

Finally, Lemma 3 is applied with $k = s$, $q = m$, and $d = \Pi_{i \in I} p_i$. This yields

$$D_m^{(s)} < \frac{s}{m} + \frac{1}{m} \sum_{\substack{I \subset \{1,\ldots,r\} \\ |I| < r}} \prod_{i \notin I} B_i \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s$$

$$< \frac{1}{m} \sum_{I \subset \{1,\ldots,r\}} \prod_{i \notin I} B_i \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s$$

$$= \frac{1}{m} \prod_{i=1}^{r} (B_i + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s,$$

which completes the proof. ■

THEOREM 2. *Suppose that* $|S_i(\tilde{\mathbf{h}})| \leq B_i$ *for any* $\tilde{\mathbf{h}} \in \mathbb{Z}^{s+1}$ *with* $\tilde{\mathbf{h}} \not\equiv \mathbf{0} \pmod{p_i}$ *and* $1 \leq i \leq r$. *Then the discrepancy* $D_N^{(s)}$ *of s-tuples (over parts of the period) in the compound method satisfies*

$$D_N^{(s)} < \frac{1}{N} \prod_{i=1}^{r} (B_i + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

for $1 \leq N < m$.

Proof. First, Lemma 2 is applied with $k = s$, $q = m$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < m$. This yields

$$D_N^{(s)} \leq \frac{m}{N} D_m(\tilde{\mathbf{x}}_0, \tilde{\mathbf{x}}_1, \ldots, \tilde{x}_{m-1}).$$

Now, Lemma 1 is applied with $k = s + 1$, $N = q = m$, and $\mathbf{t}_n = \tilde{\mathbf{x}}_n$ for $0 \leq n < m$, which implies that

$$D_N^{(s)} \leq \frac{s+1}{N} + \frac{1}{N} \sum_{\tilde{\mathbf{h}} \in C_{s+1}(m)} \frac{1}{r(\tilde{\mathbf{h}}, m)} \left| \sum_{n=0}^{m-1} e(\tilde{\mathbf{h}} \cdot \tilde{\mathbf{x}}_n) \right|$$

$$= \frac{s+1}{N} + \frac{1}{N} \sum_{\tilde{\mathbf{h}} \in C_{s+1}(m)} \frac{1}{r(\tilde{\mathbf{h}}, m)} |S(\tilde{\mathbf{h}})|$$

$$= \frac{s+1}{N} + \frac{1}{N} \sum_{\tilde{\mathbf{h}} = (\mathbf{h}, h_{s+1}) \in C_{s+1}(m)} \frac{1}{r(\tilde{\mathbf{h}}, m)} \prod_{i=1}^{r} |S_i(\mathbf{h}, h_{s+1} q_i)|,$$

where the last equality follows from Lemma 4. Hence, one obtains

$$D_N^{(s)} \le \frac{s+1}{N} + \frac{1}{N} \sum_{\substack{I \subset \{1,\dots,r\} \\ |I|<r}} \sum_{\substack{\mathbf{h}=(\mathbf{h},h_{s+1}) \in C_{s+1}(m) \\ \mathbf{h} \equiv 0 \pmod{p_i},\ i \in I \\ \mathbf{h} \not\equiv 0 \pmod{p_i},\ i \notin I}} \frac{1}{r(\tilde{\mathbf{h}}, m)} \prod_{i=1}^{r} |S_i(\mathbf{h}, h_{s+1} q_i)|$$

$$\le \frac{s+1}{N} + \frac{1}{N} \sum_{\substack{I \subset \{1,\dots,r\} \\ |I|<r}} \prod_{i \in I} p_i \prod_{i \notin I} B_i \sum_{\substack{\mathbf{h} \in C_{s+1}(m) \\ \mathbf{h} \equiv 0 \pmod{p_i},\ i \in I \\ \mathbf{h} \not\equiv 0 \pmod{p_i},\ i \notin I}} \frac{1}{r(\tilde{\mathbf{h}}, m)}$$

$$\le \frac{s+1}{N} + \frac{1}{N} \sum_{\substack{I \subset \{1,\dots,r\} \\ |I|<r}} \prod_{i \in I} p_i \prod_{i \notin I} B_i \sum_{\substack{\mathbf{h} \in C_{s+1}(m) \\ \mathbf{h} \equiv 0 \pmod{p_i},\ i \in I}} \frac{1}{r(\tilde{\mathbf{h}}, m)}.$$

Finally, Lemma 3 can be applied with $k = s + 1$, $q = m$, and $d = \Pi_{i \in I} p_i$. This yields

$$D_N^{(s)} < \frac{s+1}{N} + \frac{1}{N} \sum_{\substack{I \subset \{1,\dots,r\} \\ |I|<r}} \prod_{i \notin I} B_i \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^{s+1}$$

$$< \frac{1}{N} \sum_{I \subset \{1,\dots,r\}} \prod_{i \notin I} B_i \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^{s+1}$$

$$= \frac{1}{N} \prod_{i=1}^{r} (B_i + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^{s+1},$$

which completes the proof. ■

5. Applications

5.1. *General Nonlinear Congruential Method*

The general nonlinear congruential method (with prime modulus) has been analyzed in [3, 10, 13]. It turned out that the generated pseudorandom numbers have attractive equidistribution and statistical independence properties. However, an implementation in multiprecision of these pseudorandom number generators is usually necessary. Therefore, the compound version of the nonlinear congruential method, which overcomes this disadvantage, has been introduced in [7].

Let $i \in \{1, \dots, r\}$ and $g_i: \mathbb{Z} \to \mathbb{Z}_{p_i}$ be a permutation polynomial of $\mathbb{Z}_{p_i}$ with degree d_i as a polynomial over $\mathbb{Z}_{p_i}$, where $3 \le d_i \le p_i - 2$ is assumed in order to avoid uninteresting cases. Now, in the compound method the

sequence $(y_n^{(i)})_{n\geq 0}$ of elements of $\mathbb{Z}_{p_i}$ is defined by

$$y_n^{(i)} = g_i(n), \qquad n \geq 0.$$

In the following two results, upper bounds for the discrepancy of s-tuples of corresponding *compound nonlinear congruential pseudorandom numbers* over the full period and over parts of the period are established. Corollary 1 is a slight generalization of [7, Thm. 1].

COROLLARY 1. *Let $s \leq \min\{d_1, \ldots, d_r\}$. Then the discrepancy $D_m^{(s)}$ of s-tuples (over the full period) in the compound nonlinear congruential method satisfies*

$$D_m^{(s)} < \prod_{i=1}^{r} (d_i - 1 + p_i^{-1/2})\, m^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s.$$

Proof. First, based on a classical bound of A. Weil (cf. [12, Thm. 5.38]), it follows from [10, Proof of Thm. 1; 13, Proof of Thm. 1] that

$$|S_i(\mathbf{h}, 0)| \leq (d_i - 1)p_i^{1/2}$$

for any $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$, $s \leq d_i$, and $1 \leq i \leq r$. Hence, Theorem 1 can be applied with $B_i = (d_i - 1)p_i^{1/2}$ for $1 \leq i \leq r$. This yields

$$D_m^{(s)} < \frac{1}{m} \prod_{i=1}^{r} ((d_i - 1)p_i^{1/2} + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s$$

$$= \prod_{i=1}^{r} (d_i - 1 + p_i^{-1/2})\, m^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s$$

for $s \leq \min\{d_1, \ldots, d_r\}$. ∎

COROLLARY 2. *Let $s < \min\{d_1, \ldots, d_r\}$. Then the discrepancy $D_N^{(s)}$ of s-tuples (over parts of the period) in the compound nonlinear congruential method satisfies*

$$D_N^{(s)} < \prod_{i=1}^{r} (d_i - 1 + p_i^{-1/2}) \frac{m^{1/2}}{N} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

for $1 \leq N < m$.

Proof. It follows from [10, Proof of Thm. 2] that

$$|S_i(\tilde{\mathbf{h}})| \leq (d_i - 1)p_i^{1/2}$$

for any $\tilde{\mathbf{h}} \in \mathbb{Z}^{s+1}$ with $\tilde{\mathbf{h}} \not\equiv \mathbf{0} \pmod{p_i}$, $s < d_i$, and $1 \le i \le r$. Hence, an application of Theorem 2 with $B_i = (d_i - 1)p_i^{1/2}$ for $1 \le i \le r$ implies that

$$D_N^{(s)} < \frac{1}{N} \prod_{i=1}^{r} ((d_i - 1)p_i^{1/2} + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

$$= \prod_{i=1}^{r} (d_i - 1 + p_i^{-1/2}) \frac{m^{1/2}}{N} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

for $s < \min\{d_1, \ldots, d_r\}$ and $1 \le N < m$. ■

Let the number r of prime factors of m be fixed. Then Corollary 1 shows that $D_m^{(s)} = O(m^{-1/2}(\log m)^s)$ for $s \le \min\{d_1, \ldots, d_r\}$ and any sequence of compound nonlinear congruential pseudorandom numbers. It should be observed that this bound is independent of the specific choice of the underlying permutation polynomials $g_1, \ldots, g_r$ (with fixed degrees $d_1, \ldots, d_r$, respectively) in the compound nonlinear congruential method. The order of magnitude of the upper bound fits well the discrepancy of m true random points in $[0, 1)^s$, which is almost always of an order of magnitude $m^{-1/2}(\log \log m)^{1/2}$ according to the law of the iterated logarithm for discrepancies [1, 11]. Corollary 2 provides additional information on the quality of compound nonlinear congruential pseudorandom numbers, since it shows that $D_N^{(s)} = O(N^{-1}m^{1/2}(\log m)^{s+1})$ for $s < \min\{d_1, \ldots, d_r\}$ and $1 \le N < m$. Hence, the upper bound for the discrepancy $D_N^{(s)}$ over sufficiently large parts of the period is basically in accordance with the law of the iterated logarithm.

5.2. *Explicit Inversive Congruential Method*

The explicit inversive congruential method (with prime modulus) is a particularly promising nonlinear congruential approach, which has been studied in [6, 9, 16, 20]. The compound version of the explicit inversive congruential method has been introduced in [4].

Let $i \in \{1, \ldots, r\}$, $a_i \in \mathbb{Z}_{p_i}\backslash\{0\}$, and $b_i \in \mathbb{Z}_{p_i}$. Now, in the compound method the sequence $(y_n^{(i)})_{n \ge 0}$ of elements of $\mathbb{Z}_{p_i}$ is defined by

$$y_n^{(i)} \equiv (a_i n + b_i)^{-1} \pmod{p_i}, \qquad n \ge 0,$$

where z^{-1} denotes the multiplicative inverse of z in $\mathbb{Z}_{p_i}\backslash\{0\}$ and the abbreviation $0^{-1} = 0$ is used. In the following two results, upper bounds for the discrepancy of s-tuples of corresponding *compound explicit inversive congruential pseudorandom numbers* over the full period and over parts of the period are established. Corollary 3 slightly improves the upper bound in [4, Thm. 1].

COROLLARY 3. *The discrepancy $D_m^{(s)}$ of s-tuples (over the full period) in the compound explicit inversive congruential method satisfies*

$$D_m^{(s)} < \prod_{i=1}^{r} (2s - 2 + (s + 2)p_i^{-1/2})\, m^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s.$$

Proof. First, based on bounds for rational exponential sums, it follows from [6, Lemma 5; 9, Thm. 1; 16, Proof of Thm. 2; 20, Proof of Thm. 2] that

$$|S_i(\mathbf{h}, 0)| \le (2s - 2)p_i^{1/2} + s + 1$$

for any $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ and $1 \le i \le r$. Hence, Theorem 1 can be applied with $B_i = (2s - 2)p_i^{1/2} + s + 1$ for $1 \le i \le r$. This yields

$$D_m^{(s)} < \frac{1}{m} \prod_{i=1}^{r} ((2s - 2)p_i^{1/2} + s + 2) \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s$$

$$= \prod_{i=1}^{r} (2s - 2 + (s + 2)p_i^{-1/2})\, m^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^s. \quad \blacksquare$$

COROLLARY 4. *The discrepancy $D_N^{(s)}$ of s-tuples (over parts of the period) in the compound explicit inversive congruential method satisfies*

$$D_N^{(s)} < \prod_{i=1}^{r} (2s + (s + 1)p_i^{-1/2}) \frac{m^{1/2}}{N} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

for $1 \le N < m$.

Proof. It follows from [16, Proof of Thm. 3; 20, Proof of Thm. 3] that

$$|S_i(\tilde{\mathbf{h}})| \le 2sp_i^{1/2} + s$$

for any $\tilde{\mathbf{h}} \in \mathbb{Z}^{s+1}$ with $\tilde{\mathbf{h}} \not\equiv \mathbf{0} \pmod{p_i}$ and $1 \le i \le r$. Hence, an application of Theorem 2 with $B_i = 2sp_i^{1/2} + s$ for $1 \le i \le r$ implies that

$$D_N^{(s)} < \frac{1}{N} \prod_{i=1}^{r} (2sp_i^{1/2} + s + 1) \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

$$= \prod_{i=1}^{r} (2s + (s + 1)p_i^{-1/2}) \frac{m^{1/2}}{N} \left(\frac{2}{\pi} \log m + \frac{7}{5}\right)^{s+1}$$

for $1 \le N < m$. $\blacksquare$

Let the number r of prime factors of m be fixed. Then Corollary 3 shows that $D_m^{(s)} = O(m^{-1/2}(\log m)^s)$ for any sequence of compound explicit inversive congruential pseudorandom numbers, where the implied constant is absolute. It should be observed that this bound is independent of the specific choice of the parameters in the compound explicit inversive congruential method. The order of magnitude of the upper bound fits well the discrepancy of m true random points in $[0, 1)^s$, which is almost always of an order of magnitude $m^{-1/2}(\log \log m)^{1/2}$ according to the law of the iterated logarithm for discrepancies [1, 11]. Corollary 4 provides additional information on the quality of compound explicit inversive congruential pseudorandom numbers, since it shows that $D_N^{(s)} = O(N^{-1}m^{1/2}(\log m)^{s+1})$ for $1 \le N < m$. Hence, the upper bound for the discrepancy $D_N^{(s)}$ over sufficiently large parts of the period is basically in accordance with the law of the iterated logarithm.

ACKNOWLEDGMENT

The author thanks the referees for their valuable comments.

REFERENCES

1. K. L. Chung, An estimate concerning the Kolmogoroff limit distribution, *Trans. Amer. Math. Soc.* **67** (1949), 36–50.
2. J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers: A tutorial, *Internat. Statist. Rev.* **60** (1992), 167–176.
3. J. Eichenauer-Herrmann, Equidistribution properties of nonlinear congruential pseudorandom numbers, *Metrika* **40** (1993), 333–338.
4. J. Eichenauer-Herrmann, Explicit inversive congruential pseudorandom numbers: The compound approach, *Computing* **51** (1993), 175–182.
5. J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers, *Z. Angew. Math. Mech.* **73** (1993), T644–T647.
6. J. Eichenauer-Herrmann, Statistical independence of a new class of inversive congruential pseudorandom numbers, *Math. Comp.* **60** (1993), 375–384.
7. J. Eichenauer-Herrmann, Compound nonlinear congruential pseudorandom numbers, *Monatsh. Math.* **117** (1994), 213–222.
8. J. Eichenauer-Herrmann, Pseudorandom number generation by nonlinear methods, *Internat. Statist. Rev.*, to appear.
9. J. Eichenauer-Herrmann and H. Niederreiter, Bounds for exponential sums and their applications to pseudorandom numbers, *Acta Arith.*, to appear.
10. J. Eichenauer-Herrmann and H. Niederreiter, On the statistical independence of nonlinear congruential pseudorandom numbers, *ACM Trans. Modeling Computer Simulation*, to appear.
11. J. Kiefer, On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm, *Pacific J. Math.* **11** (1961), 649–660.

12. R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, Reading, MA, 1983.
13. H. Niederreiter, Statistical independence of nonlinear congruential pseudorandom numbers, *Monatsh. Math.* **106** (1988), 149–159.
14. H. Niederreiter, Recent trends in random number and random vector generation, *Ann. Oper. Res.* **31** (1991), 323–346.
15. H. Niederreiter, Finite fields, pseudorandom numbers, and quasirandom points, *in* "Finite Fields, Coding Theory, and Advances in Communications and Computing" (G. L. Mullen and P. J.-S. Shiue, Eds.), pp. 375–394, Dekker, New York, 1992.
16. H. Niederreiter, New methods for pseudorandom number and pseudorandom vector generation, *in* "Proc. 1992 Winter Simulation Conf.," pp. 264–269, IEEE Press, Piscataway, NJ, 1992.
17. H. Niederreiter, Nonlinear methods for pseudorandom number and vector generation, *in* "Simulation and Optimization" (G. Pflug and U. Dieter, Eds.), Lecture Notes in Econom. and Math. Systems, Vol. 374, pp. 145–153, Springer, Berlin, 1992.
18. H. Niederreiter, "Random Number Generation and Quasi-Monte Carlo Methods," SIAM, Philadelphia, 1992.
19. H. Niederreiter, Pseudorandom numbers and quasirandom points, *Z. Angew. Math. Mech.* **73** (1993), T648–T652.
20. H. Niederreiter, On a new class of pseudorandom numbers for simulation methods, *J. Comput. Appl. Math.*, to appear.
21. B. A. Wichmann and I. D. Hill, An efficient and portable pseudo-random number generator, *Appl. Statist.* **31** (1982), 188–190.